ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Засоби захисту кінцевих пристроїв в інформаційній системі організації на базі CISCO ASA»

зі спеціальності *125 Кібербезпека*
(код, найменування спеціальності)

освітньо-професійної програми *Інформаційна та кібернетична безпека*
(назва програми)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Володимир ШАРПІТА
(підпис)

Виконав: здобувач вищої освіти групи БСД-44
ШАРПІТА Володимир
(прізвище, ім'я)

Керівник асистент, Бойко Анна
(науковий ступінь, вчене звання, прізвище, ім'я)

Рецензент _____
(науковий ступінь, вчене звання, прізвище, ім'я)

Київ 2025

ВСТУП

Актуальність дослідження. Захист кінцевих пристроїв є важливим аспектом забезпечення безпеки в будь-якій організації. Кінцеві пристрої, такі як комп'ютери, мобільні телефони, ноутбуки, є основними точками доступу до корпоративних даних і мереж. Враховуючи постійне зростання кількості кіберзагроз та атак на ці пристрої, захист кінцевих точок стає критично важливим для запобігання витоку даних і забезпечення цілісності інформації в організації. Незахищені кінцеві пристрої можуть стати вразливими для різноманітних атак, таких як шкідливе програмне забезпечення, фішинг та експлойти.

Оскільки більшість сучасних кіберзагроз спрямовані на кінцеві пристрої, їх захист має вирішальне значення для забезпечення загальної безпеки організації. Одним з ефективних способів захисту кінцевих пристроїв є інтеграція системи захисту кінцевих точок з міжмережевим екраном, таким як Cisco ASA. Це дозволяє забезпечити комплексну безпеку, контролюючи трафік, що надходить до мережі, і забезпечуючи захист від потенційних загроз на рівні кінцевих точок.

Мета роботи: аналіз та розробка методів і засобів захисту кінцевих пристроїв в організації на основі Cisco ASA.

Наукові завдання:

- Оцінка ролі Cisco ASA в забезпеченні безпеки кінцевих пристроїв.
- Розробка стратегії інтеграції Cisco ASA з іншими засобами захисту кінцевих пристроїв, такими як рішення для виявлення шкідливого ПЗ і моніторингу загроз.
- Аналіз можливостей Cisco ASA для контролю доступу до корпоративної мережі та фільтрації трафіку.
- Розробка рекомендацій щодо оптимізації використання Cisco ASA для підвищення безпеки кінцевих пристроїв.

Об'єкт дослідження – це процес захисту кінцевих пристроїв в організації.

Предмет дослідження – методи та засоби захисту кінцевих пристроїв організації на базі Cisco ASA.

Методи дослідження. В дослідженні будуть використані методи аналізу існуючих рішень з кібербезпеки, дослідження документації Cisco ASA, порівняльний аналіз ефективності різних засобів захисту кінцевих точок та їх інтеграція з іншими рішеннями Cisco.

Практичне значення одержаних результатів. Розроблені рекомендації щодо застосування Cisco ASA для забезпечення безпеки кінцевих пристроїв допоможуть організаціям покращити рівень захисту своїх кінцевих точок і мережі в цілому. Інтеграція Cisco ASA з іншими засобами захисту забезпечить більш комплексний підхід до безпеки, що дозволить швидко реагувати на нові загрози, знижувати ризики витоку даних і забезпечити стабільну роботу корпоративної мережі навіть у разі виявлення інцидентів

1 АНАЛІЗ ПРОБЛЕМИ ЗАХИСТУ КІНЦЕВИХ ТОЧОК ОРГАНІЗАЦІЇ

1.1. Аналіз актуальних загроз для кінцевих точок в інформаційних системах

Кінцеві точки (endpoints) є ключовими компонентами будь-якої інформаційної системи, через які користувачі взаємодіють із мережею та отримують доступ до корпоративних ресурсів. До таких кінцевих точок належать різноманітні пристрої – комп'ютери, ноутбуки, мобільні телефони, планшети, а також інші електронні гаджети, які підключаються до корпоративної мережі або Інтернету. Через свою природу кінцеві точки є одними з найвразливіших місць у системі безпеки, адже саме через них може відбуватися несанкціонований доступ або компрометація інформації. Захист цих точок має першочергове значення для підтримки цілісності, конфіденційності та доступності даних в організації.

Однією з найбільших загроз, що впливають на кінцеві точки, є шкідливе програмне забезпечення, або malware. Цей термін охоплює широкий спектр небезпечних програмних продуктів, серед яких віруси, трояни, шпигунські програми, руткіти, криптовіруси та інші типи зловмисних програм, що можуть пошкоджувати або викрадати дані. Основні шляхи проникнення malware на кінцеві пристрої – це фішингові електронні листи, заражені веб-сайти, а також використання зовнішніх носіїв інформації, таких як USB-флешки, які не проходять належного контролю. Потрапивши на пристрій, шкідливе програмне забезпечення може викрадати конфіденційну інформацію, руйнувати файли, забезпечувати зловмисникам несанкціонований доступ до систем або навіть повністю блокувати роботу пристрою, що становить велику загрозу для безпеки організації.

Ще однією серйозною і поширеною загрозою є фішинг – метод соціальної інженерії, що полягає у введенні користувачів в оману за допомогою підроблених електронних листів, веб-сайтів або мобільних додатків. Зловмисники створюють зовні правдоподібні підробки офіційних ресурсів – банківських сайтів,

корпоративних порталів або сервісів, що викликають довіру. Вони можуть надсилати листи із закликами терміново оновити пароль, підтвердити особисті дані або перейти за посиланням, що веде на фальшивий сайт, де відбувається викрадення облікових даних. Іноді фішинг здійснюється навіть через телефонні дзвінки, коли злочинці видають себе за працівників банку або служби підтримки. У результаті користувачі надають інформацію, таку як логіни, паролі, номери кредитних карток чи доступи до корпоративних акаунтів, що може призвести до значних збитків і порушення безпеки системи.

Крім того, використання вразливостей програмного забезпечення є ще однією поширеною загрозою. Програми та операційні системи часто мають невиправлені вразливості, які можуть бути використані хакерами для несанкціонованого доступу до кінцевої точки. Якщо програмне забезпечення не оновлюється своєчасно, відомі уразливості можуть стати основним каналом для атак, включаючи віддалене виконання коду або доступ до локальних файлів. Зловмисники можуть використати ці вразливості для проникнення в систему, крадіжки або модифікації даних.

Загроза для мобільних пристроїв зростає з кожним роком, оскільки ці пристрої все більше використовуються для роботи з чутливою інформацією. Мобільні пристрої часто мають слабший рівень безпеки порівняно з десктопними комп'ютерами, що робить їх вразливими до атак. Мобільні додатки можуть бути заражені шкідливим програмним забезпеченням або використані для фішингових атак. Окрім того, мобільні пристрої часто підключаються до незахищених мереж Wi-Fi або використовують небезпечні знімні носії, що ще більше підвищує ризики.

Сучасна кіберзлочинність використовує дедалі витонченіші підходи до компрометації кінцевих пристроїв, зокрема поєднуючи технічні засоби з методами соціальної інженерії. Від фішингу та експлуатації вразливостей до застосування безфайлових атак – спектр загроз постійно розширюється, що вимагає від організацій не лише впровадження стандартних засобів захисту, а й активного аналізу та адаптації до нових сценаріїв атак.

Однією з ключових тенденцій є поширення цільових атак, орієнтованих саме на кінцеві точки користувачів, як найменш захищені компоненти мережі. Такі атаки можуть включати попередню розвідку, розгортання бекдорів, а також використання легітимного ПЗ для прихованого управління пристроєм жертви. Особливо небезпечними є атаки нульового дня, які використовують ще не виправлені вразливості операційних систем і популярних додатків.

Усе більш актуальним стає захист мобільних кінцевих пристроїв, які використовуються для доступу до корпоративних систем у гібридному або віддаленому режимі. Вони часто не покриваються традиційними інструментами безпеки, такими як класичні антивіруси чи мережеві фаєрволи, і потребують використання спеціалізованих рішень, таких як UEM (Unified Endpoint Management) та контейнеризація даних.

Не менш значущим є аспект використання легітимного ПЗ для зловмисних цілей (так звані living-off-the-land атаки), коли зловмисники використовують штатні системні інструменти (наприклад, PowerShell або WMI) для розгортання шкідливого функціоналу без завантаження додаткових файлів, що ускладнює виявлення таких атак традиційними методами.

З огляду на це, стає очевидним, що для ефективного захисту кінцевих точок замало лише застосовувати антивіруси чи фаєрволи. Необхідно впроваджувати багаторівневу модель захисту, яка передбачає постійний моніторинг активності, поведінковий аналіз, контроль доступу та шифрування даних. Важливою складовою такої моделі є застосування рішень EDR/XDR (Endpoint Detection and Response / Extended Detection and Response), які дозволяють виявляти та нейтралізовувати складні атаки на основі аномальної поведінки систем і користувачів.

Таким чином, сучасні загрози вимагають від організацій переходу від реактивного до прогнозувального підходу, де проактивний аналіз і постійне вдосконалення засобів захисту є обов’язковими умовами підтримки безпеки кінцевих точок.

1.2. Аналіз підходів до захисту кінцевих точок в корпоративному середовищі

У сучасному корпоративному середовищі кінцеві точки – це не лише робочі станції та сервери, а й мобільні пристрої, IoT-девайси та віртуальні машини. З огляду на тенденцію до гібридної роботи та зростання кількості підключених пристроїв, захист кінцевих точок (Endpoint Protection) стає критично важливим елементом кібербезпеки.

В табл. 1.2 показано види кінцевих точок, їх особливості та можливі для них загрози

Табл. 1.2

Види кінцевих точок, їх особливості та можливі для них загрози

Види кінцевих точок	Особливості	Можливі загрози
Робочі станції (ПК, ноутбуки)	Найпоширеніші пристрої з постійним доступом до мережі; можуть зберігати критичні дані	Фішинг, зловмисне ПЗ (віруси, трояни), експлуатація вразливостей ОС та додатків, витік даних
Мобільні пристрої (смартфони, планшети)	Підключаються до корпоративної мережі, часто використовують незахищені мережі	Встановлення шкідливих додатків, перехоплення даних через незахищені Wi-Fi, втрати/крадіжки
Сервери (фізичні, віртуальні)	Обробляють велику кількість запитів, часто є цілями для атак з високим впливом	DDoS, експлуатація вразливостей, несанкціонований доступ, шкідливі скрипти
Пристрої IoT (камери, датчики, побутові пристрої)	Обмежені ресурси, часто не мають належного захисту	Вбудовані бекдори, ботнети (напр. Mirai), небезпека через відсутність оновлень
Тонкі клієнти / VDI (віртуальні робочі місця)	Централізоване управління, менше даних зберігається локально	Атаки на сервер віртуалізації, вразливості протоколів підключення, міжкористувацьке шпигування

Продовження табл. 1.2

Види кінцевих точок	Особливості	Можливі загрози
USB-накопичувачі, зовнішні носії	Переносні, використовуються для швидкого обміну даними	Інфікування вірусами, крадіжка інформації, несвідоме поширення шкідливого ПЗ
Термінали обслуговування (банкомати, POS-системи)	Використовуються у фінансових та торгових мережах, часто мають обмежене ПЗ	Фізичні атаки, скімінг, експлуатація вразливостей у ПЗ, доступ до даних карт

Розглянемо основні підходи та технології, що застосовуються для цього захисту.

Традиційні антивірусні програми використовують сигнатурний аналіз для виявлення відомих загроз. Однак вони мають обмежену здатність протидіяти новим або невідомим атакам.

EPP – це рішення, які забезпечують базовий захист від вірусів, шкідливого програмного забезпечення, фішингу та несанкціонованого доступу. Вони включають функції, такі як брандмауери, виявлення вторгнень та контроль доступу.

EDR – системи надають розширені можливості моніторингу, виявлення та реагування на загрози в реальному часі. Вони використовують аналіз поведінки, машинне навчання та централізоване зберігання даних для виявлення складних атак.

XDR – інтегрує дані з різних джерел, таких як мережі, сервери та хмарні середовища, для забезпечення комплексного захисту. Це дозволяє виявляти та реагувати на загрози на різних рівнях інфраструктури.

Zero Trust – передбачає, що жоден пристрій або користувач не повинен автоматично довірятися. Кожен запит на доступ перевіряється та аутентифікується,

незалежно від того, чи знаходиться користувач всередині чи за межами корпоративної мережі.

EPM – обмежує доступ користувачів до систем та даних відповідно до їхніх ролей. Це зменшує ризик несанкціонованого доступу та поширення атак у разі компрометації кінцевої точки.

Поведінкова безпека використовує аналіз аномальної активності для виявлення потенційних загроз. Це дозволяє виявляти нові або модифіковані атаки, які можуть уникати традиційних методів виявлення.

Регулярне оновлення програмного забезпечення та операційних систем є ключовим аспектом захисту кінцевих точок. Автоматизоване управління патчами допомагає зменшити ризик використання відомих вразливостей.

Навчання співробітників основам кібергігієни та розпізнаванню фішингових атак знижує ймовірність успішних соціальних атак.

Інтеграція EDR з іншими системами безпеки, такими як SIEM (Security Information and Event Management) та SOAR (Security Orchestration, Automation, and Response), дозволяє автоматизувати реагування на інциденти та покращити ефективність захисту.

Захист кінцевих точок є багаторівневим процесом, що вимагає інтеграції різних технологій та підходів. Вибір відповідних рішень залежить від специфіки організації, її інфраструктури та рівня загроз. Сучасні рішення, такі як EDR та XDR, забезпечують гнучкий та ефективний захист, відповідаючи на виклики сучасного кіберпростору.

Для забезпечення ефективного захисту кінцевих точок необхідно впроваджувати комплексні стратегії реагування на інциденти безпеки. Незважаючи на всі зусилля з попередження атак, деякі загрози можуть проникати в систему, тому потрібно мати чітко визначені плани дій у разі інцидентів. Ці плани включають послідовність етапів – від виявлення інциденту, аналізу його характеру, оперативного реагування до відновлення нормального функціонування системи. Швидке реагування дозволяє мінімізувати шкоду, яку можуть завдати

зловмисники, та скоротити час, протягом якого вони можуть контролювати систему чи отримувати доступ до конфіденційної інформації.

Один із ключових аспектів такої стратегії – безперервне вдосконалення заходів безпеки на основі аналізу попередніх інцидентів і атак. Постійний аудит вразливостей кінцевих точок, моніторинг змін у методах атак кіберзлочинців та проведення регулярних тестів на проникнення (penetration tests) дають змогу виявити слабкі місця системи до того, як ними скористаються зловмисники. Такий проактивний підхід допомагає підтримувати високий рівень захисту.

Ключовою складовою є використання систем моніторингу безпеки кінцевих пристроїв у режимі реального часу. Ці системи аналізують поведінку користувачів і додатків, виявляють аномальні чи підозрілі дії, що можуть свідчити про початок атаки чи компрометацію системи. Завдяки цьому можна оперативно виявляти нові види шкідливого програмного забезпечення, фішингові спроби або інші загрози і вчасно вживати заходів для їх нейтралізації.

Ще одним принциповим елементом є інтеграція захисту кінцевих точок із загальною системою безпеки організації. Взаємодія з платформами управління подіями безпеки (SIEM) та системами запобігання вторгненням (IDS/IPS) дозволяє централізовано збирати та аналізувати дані з різних джерел. Це значно покращує здатність системи виявляти складні, багатоетапні атаки і забезпечує швидке і скоординоване реагування на них [14].

Загалом, ефективний захист кінцевих точок – це безперервний і комплексний процес, який передбачає не лише впровадження сучасних технологічних рішень, але й постійне навчання та підвищення обізнаності персоналу. Організації, що інтегрують сучасні засоби захисту, моніторинг та плани реагування, можуть значно знизити ймовірність успішних атак, зберегти конфіденційність та цілісність своїх даних, а також забезпечити безперебійну роботу своїх інформаційних систем.

Ключовим елементом такого підходу є постійний моніторинг і виявлення загроз у реальному часі за допомогою систем EDR, які аналізують поведінку пристроїв і користувачів, застосовуючи технології машинного навчання для

розпізнавання нових складних атак. Це дозволяє мінімізувати вплив кібератак і забезпечити більш ефективний захист організації.

Інтеграція різних платформ безпеки, таких як SIEM, SOAR та інших систем оркестрування безпеки, сприяє централізованому управлінню інформацією про загрози та координації реагування на інциденти. Водночас застосування методів управління доступом і шифрування даних дозволяє знизити ризики несанкціонованого доступу до критичної інформації.

Необхідно також забезпечувати регулярне оновлення програмного забезпечення та оперативно реагувати на зміни у тактиках і методах кіберзлочинців. Підвищення рівня обізнаності співробітників щодо кібергігієни, фішингових атак та основ інформаційної безпеки є необхідною умовою для побудови стійкої системи захисту кінцевих точок.

Отже, успішний захист кінцевих пристроїв базується на комплексній інтеграції технологічних засобів, постійному моніторингу загроз та безперервному навчанні персоналу. Такий підхід дозволяє значно знизити ризики кіберінцидентів і забезпечити надійний захист інформаційних систем та даних організації.

Окрім цього, слід враховувати, що захист кінцевих точок – це не лише технічне завдання, але й організаційне питання. Впровадження чітких політик безпеки, процедур реагування на інциденти, а також навчання персоналу є ключовими факторами для забезпечення ефективної роботи системи захисту. Регулярні тренінги та підвищення обізнаності співробітників щодо найкращих практик кібербезпеки допомагають мінімізувати людський фактор, який часто є слабким місцем у загальній системі захисту.

Доцільно звернути увагу на тестування та перевірки надійності систем захисту кінцевих точок. Регулярні аудитори безпеки, проведення пенетраційних тестів та моделювання атак допомагають виявити недоліки у конфігураціях, що може стати основою для подальшого вдосконалення захисних заходів.

Інтеграція з хмарними сервісами та мобільними пристроями, які все частіше використовуються в сучасних організаціях, вимагає гнучких і масштабованих рішень для захисту кінцевих точок. Використання рішень, які підтримують

багатоплатформенність і мають можливість централізованого управління, дозволяє організаціям підтримувати безпеку у різних IT-середовищах.

Нарешті, дотримання стандартів і нормативних вимог, таких як GDPR або ISO 27001, є пріоритетною складовою захисту кінцевих точок. Впровадження відповідних технологічних і організаційних заходів допомагає не лише забезпечити безпеку, а й уникнути штрафів та зберегти довіру клієнтів і партнерів.

Таким чином, ефективний захист кінцевих точок – це безперервний і комплексний процес, що охоплює технічні, організаційні та нормативні аспекти. Лише системний підхід, що поєднує сучасні технології, навчання персоналу і відповідальне управління, здатен забезпечити належний рівень безпеки в умовах постійно змінюваного кіберпростору.

1.3 Огляд існуючих рішень для захисту кінцевих пристроїв

У 2025 році ринок рішень для захисту кінцевих пристроїв (Endpoint Protection) пропонує широкий спектр інструментів, здатних ефективно протидіяти сучасним кіберзагрозам. Ось огляд кількох провідних рішень, що здобули високі оцінки за ефективність, інноваційність та зручність використання.

SentinelOne Singularity Endpoint Security – це хмарна платформа, що поєднує функції EDR, XDR та AI-орієнтованого реагування на загрози. Платформа була відзначена як лідер у Gartner Magic Quadrant 2024 року. Крім того, вона має співпрацю з Lenovo для інтеграції безпеки на основі AI в пристрої ThinkShield. Платформа має високу ефективність у виявленні загроз, швидке реагування та масштабується для великих підприємств.

CrowdStrike Falcon – це також хмарна платформа з передовими можливостями EDR та XDR. Використовує AI для покращення ефективності виявлення загроз. Платформа отримала високу оцінку від Gartner і забезпечує глибокий аналіз загроз та інтеграцію з іншими рішеннями безпеки. Незважаючи на це, у липні 2024 року сталася глобальна перерва в роботі через помилку оновлення.

Sophos Intercept X – це рішення поєднує захист від програм-вимагачів, глибоке навчання для виявлення шкідливого ПЗ, а також підтримку EDR та XDR. Його визнано лідером у Gartner Magic Quadrant 2024 року та отримало високі оцінки від AV-Comparatives та SE Labs. Інтерфейс є інтуїтивно зрозумілим, а можливості відновлення після атак ефективні. Крім того, платформа інтегрується з іншими рішеннями безпеки [13].

Microsoft Defender for Endpoint – це інтегроване рішення в екосистему Microsoft 365, що надає можливості EDR та XDR, а також захист від витоків даних. Його перевагою є глибока інтеграція з іншими продуктами Microsoft, зручність управління та автоматизація реагування на інциденти.

ESET Endpoint Security – це рішення з модульною архітектурою, яке забезпечує підтримку EDR, захист від програм-вимагачів та фаєрвол. Воно є ефективним для малих та середніх підприємств, де потрібна легкість управління та низьке споживання ресурсів. Однак воно не має деяких розширених функцій для великих організацій [14].

Bitdefender GravityZone – ця платформа також має централізоване управління та поєднує EDR, захист від програм-вимагачів та фаєрвол. Вона ефективно виявляє загрози, зручна у використанні та масштабується для різних розмірів організацій.

ThreatLocker Zero Trust Endpoint Protection – це рішення на основі принципу Zero Trust, яке забезпечує контроль доступу до додатків та даних. Це рішення підходить для середовищ з високими вимогами до захисту даних, надаючи високий рівень безпеки.

Вибір оптимального рішення для захисту кінцевих пристроїв залежить від потреб вашої організації. Якщо ваша організація велика або має високі вимоги до безпеки, то рішення, такі як SentinelOne або CrowdStrike Falcon, будуть ідеальними завдяки можливостям виявлення та реагування на загрози, а також інтеграції з іншими інструментами безпеки. Для малих та середніх підприємств чудово підходять ESET та Bitdefender, які пропонують ефективний захист з низьким споживанням ресурсів та простотою управління. Для організацій з високими вимогами до безпеки, особливо в умовах роботи з критичними даними,

ThreatLocker може бути оптимальним вибором завдяки застосуванню принципу Zero Trust [15].

Таким чином, для ефективного захисту кінцевих пристроїв необхідно вибрати рішення, що найбільше відповідає розмірам організації, її вимогам до безпеки та інфраструктурі.

У 2025 році ринок рішень для захисту кінцевих пристроїв пропонує широкий вибір інструментів, що забезпечують ефективний захист від сучасних кіберзагроз. Рішення, такі як SentinelOne Singularity Endpoint Security, CrowdStrike Falcon, Sophos Intercept X, Microsoft Defender for Endpoint, ESET Endpoint Security, Bitdefender GravityZone та ThreatLocker Zero Trust Endpoint Protection, мають різноманітні функціональні можливості та підходи до забезпечення безпеки кінцевих пристроїв, що дозволяє організаціям вибирати оптимальні варіанти відповідно до їхніх потреб.

Платформи на основі AI, такі як SentinelOne та CrowdStrike, забезпечують високі показники виявлення загроз і швидке реагування, що є значущими для великих підприємств з високими вимогами до безпеки. Водночас, рішення, як-от ESET та Bitdefender, є чудовими для малих та середніх підприємств завдяки простоті управління та низькому споживанню ресурсів.

Завдяки своїм розширеним можливостям інтеграції, таких як підтримка Zero Trust в ThreatLocker, ці рішення ідеально підходять для організацій, що мають високі вимоги до захисту даних і контролю доступу. Крім того, платформи, як Microsoft Defender for Endpoint, пропонують зручну інтеграцію з іншими продуктами, що робить їх ідеальним вибором для організацій, які вже використовують інфраструктуру Microsoft.

Таким чином, для ефективного захисту кінцевих пристроїв необхідно враховувати розмір організації, рівень її вимог до безпеки, а також специфіку інфраструктури. Вибір правильного рішення допоможе забезпечити належний рівень захисту від кіберзагроз та зберегти цілісність і конфіденційність даних.

На відміну від сучасних платформ для захисту кінцевих пристроїв, таких як SentinelOne, CrowdStrike Falcon або Sophos Intercept X, Cisco ASA (Adaptive

Security Appliance) не є типовим EPP/EDR/XDR-рішенням. Натомість, Cisco ASA виконує функції міжмережевого екрану, системи запобігання вторгненням (IPS/IDPS), VPN-шлюзу та базового контролю доступу, що робить його ключовим компонентом у perimeter-based моделі захисту. Проте, з розвитком концепцій Zero Trust, XDR та хмароорієнтованих підходів, постає потреба чіткого розуміння ролі ASA в сучасній архітектурі безпеки.

У порівнянні з SentinelOne або CrowdStrike Falcon, Cisco ASA не має вбудованої системи аналізу поведінки користувачів (UEBA), AI/ML-аналізу подій безпеки чи автоматизованого реагування на інциденти. Ці рішення орієнтовані на постійний моніторинг кінцевих точок і аналіз телеметрії в реальному часі, тоді як Cisco ASA більше зосереджений на контролі трафіку та ізоляції сегментів мережі.

Sophos Intercept X та Bitdefender GravityZone також пропонують багаторівневий захист, зокрема виявлення експлойтів, захист від програм-вимагачів і систему відновлення після атак. Cisco ASA, хоча і забезпечує базові функції IPS/IDS, не здатен самостійно реагувати на інциденти в середовищі кінцевих пристроїв або відновлювати пошкоджені системи, якщо не інтегрується з іншими компонентами Cisco Secure (такими як Secure Endpoint або SecureX).

Microsoft Defender for Endpoint вигідно вирізняється завдяки глибокій інтеграції в ОС Windows і Microsoft 365, що дозволяє організаціям централізовано керувати політиками безпеки, виявляти загрози та автоматизовано реагувати на них. Cisco ASA не має такого рівня взаємодії з операційними системами та програмним забезпеченням користувача – його основна перевага полягає в контролі доступу на рівні мережі, VPN-захисті та розширеному фільтруванні трафіку.

Що стосується ThreatLocker, який використовує модель Zero Trust для захисту кінцевих точок, то його принципи побудови політик доступу та виконання додатків суттєво відрізняються від підходів Cisco ASA. ASA, у класичному вигляді, не реалізує Zero Trust у повному розумінні, однак, у поєднанні з Cisco ISE (Identity Services Engine), Duo та іншими рішеннями Cisco, може слугувати частиною Zero Trust-архітектури, зокрема для мережевого рівня.

Нарешті, варто зазначити, що хоча Cisco ASA не є конкурентом платформ EDR/XDR у звичному розумінні, його використання залишається виправданим у середовищах, де важливу роль відіграє мережевий периметр, віддалений доступ через VPN, контроль міжсегментного трафіку, а також захист від зовнішніх атак. У поєднанні з сучасними агентами EDR/XDR та SIEM/SOAR-рішеннями, ASA може бути частиною глибоко ешелонованої стратегії кібербезпеки.

В табл. 1.3 продемонстровано порівняння Cisco ASA з сучасними рішеннями для захисту кінцевих пристроїв (EPP/EDR/XDR).

Табл. 1.3

Порівняльна таблиця Cisco ASA з сучасними рішеннями для захисту кінцевих пристроїв (EPP/EDR/XDR)

Характеристика / Рішення	Cisco ASA	SentinelOne / CrowdStrike Falcon	Sophos Intercept X	Microsoft Defender for Endpoint	Bitdefender / ESET	ThreatLocker Zero Trust
Тип рішення	Мережевий міжмережевий екран, VPN, IPS	EDR/XDR, AI-аналіз	EPP/EDR, захист від ransomware	EDR/XDR, інтеграція з Windows	EPP/EDR	Zero Trust EPP
Захист кінцевих точок (Endpoint)	Непряма підтримка (через трафік)	Повноцінний агент	Повноцінний агент	Повноцінний агент	Повноцінний агент	Повноцінний агент
AI/ML виявлення загроз	Відсутній	Так	Так	Так	Частково	Ні
Функції Zero Trust	Частково (через інтеграцію з ISE)	Частково	Частково	Частково	Відсутні	Основна концепція
VPN / мережевий доступ	Так (IPsec, SSL VPN)	Відсутній	Відсутній	Відсутній	Відсутній	Відсутній
Інтеграція з іншими рішеннями	З Cisco Secure, ISE, Duo, Umbrella	Так (SIEM, SOAR, інше)	Так (з Sophos Central)	Висока (з Microsoft 365)	Обмежена	Обмежена
Автоматизоване реагування на загрози (SOAR)	Ні (можливо через інтеграцію)	Так	Так	Так	Частково	Ні

Продовження табл. 1.3

Характеристика / Рішення	Cisco ASA	SentinelOne / CrowdStrike Falcon	Sophos Intercept X	Microsoft Defender for Endpoint	Bitdefender / ESET	ThreatLocker Zero Trust
Цільова аудиторія	Корпоративні мережі, VPN-доступ	Великі та середні підприємства	Усі сегменти	Організації в екосистемі Microsoft	Малі та середні підприємства	Середній та високий рівень безпеки
Переваги	Надійний контроль трафіку, VPN	AI, швидке реагування	Ransomware-захист, простота	Інтеграція з Windows	Ефективність, простота	Політика 'блокувати за замовчуванням'
Обмеження	Немає глибокого аналізу на хості	Залежність від хмари	Не повністю Zero Trust	Залежність від Microsoft	Немає глибоких аналітичних механізмів	Немає аналітики загроз

2 АРХІТЕКТУРА ТА МОЖЛИВОСТІ CISCO ASA ДЛЯ ЗАХИСТУ КІНЦЕВИХ ТОЧОК

2.1. Основні функції Cisco ASA у забезпеченні безпеки

Cisco ASA (Adaptive Security Appliance) є високопродуктивним пристроєм, який забезпечує багаторівневий захист для корпоративних мереж, поєднуючи функції міжмережевого екрану, VPN-концентратора, а також системи виявлення та запобігання вторгненням (IDS/IPS). Завдяки цьому пристрій надає надійний захист від зовнішніх та внутрішніх кіберзагроз, забезпечуючи високу ефективність і гнучкість у налаштуваннях мережевої безпеки.

Основною функцією Cisco ASA є забезпечення міжмережевого екрану, який здійснює перевірку стану з'єднань, аналізуючи пакети в контексті їхнього стану та історії з'єднань. Це дозволяє блокувати несанкціонований доступ і зловмисний трафік, забезпечуючи високий рівень безпеки. Система аналізує кожен пакет, порівнюючи його з уже існуючими з'єднаннями, що дозволяє ефективно захищати мережу від зовнішніх атак.

Cisco ASA підтримує як IPsec, так і SSL VPN, що дозволяє забезпечити безпечний віддалений доступ до корпоративної мережі для користувачів, незалежно від їхнього місцезнаходження. Це особливо потрібно в умовах гнучкої роботи і мобільності співробітників, оскільки дозволяє їм підключатися до внутрішніх мереж компанії через захищене з’єднання, що знижує ризики витоку конфіденційної інформації.

Cisco ASA інтегрується з Cisco Firepower, що дозволяє системі виявляти та блокувати атаки на рівні додатків, аналізуючи трафік на наявність шкідливих патернів і аномалій. Це забезпечує додатковий рівень безпеки, оскільки Firepower активно перевіряє весь вхідний і вихідний трафік на предмет наявності шкідливих елементів або несанкціонованих спроб вторгнення [16].

Cisco ASA дозволяє здійснювати глибокий аналіз додатків, визначаючи та контролюючи використання певних програм або сервісів у мережі. Ця функція допомагає запобігти несанкціонованому використанню ресурсів компанії, обмежуючи доступ до програм, що можуть становити загрозу для безпеки або використовувати корпоративну мережу без дозволу.

Cisco ASA інтегрована з Advanced Malware Protection (AMP), що дозволяє виявляти та блокувати відомі та невідомі загрози, використовуючи передові методи машинного навчання і аналізу поведінки. AMP дозволяє оперативно реагувати на нові загрози, що можуть з’являтися в мережі.

Моделі Cisco ASA мають модульну архітектуру, що дозволяє додавати різні модулі безпеки, такі як Firepower, для розширення функціональності пристрою залежно від змінюваних вимог безпеки. Це дає можливість адаптувати систему до нових загроз і забезпечувати високий рівень безпеки в умовах постійних змін у кіберпросторі.

Cisco ASA підтримує конфігурації високої доступності, такі як Active/Standby та Active/Active. Це дозволяє забезпечити безперервну роботу системи навіть у разі відмови одного з пристроїв. Така масштабованість дозволяє системі ефективно обробляти збільшення навантаження, зберігаючи високу продуктивність.

Cisco ASA може бути інтегрована з іншими продуктами Cisco, такими як Cisco Identity Services Engine (ISE) і Cisco Umbrella, що дозволяє забезпечити комплексний підхід до мережевої безпеки. Це дає можливість централізовано управляти політиками безпеки і забезпечити додаткові рівні захисту.

Завдяки таким функціям Cisco ASA є передовим і надійним рішенням для забезпечення захисту корпоративних мереж від різноманітних кіберзагроз. Висока гнучкість налаштувань та можливість інтеграції з іншими рішеннями роблять Cisco ASA ідеальним вибором для великих підприємств, які потребують надійної системи безпеки для захисту своїх даних і ресурсів.

Cisco ASA (Adaptive Security Appliance) є одним із найефективніших рішень для забезпечення захисту корпоративних мереж від кіберзагроз завдяки своїй

універсальності, ефективності та гнучкості. Це пристрій, який поєднує в собі кілька значущих функцій для забезпечення безпеки, таких як міжмережевий екран, VPN-концентратор та система виявлення й запобігання вторгненням (IDS/IPS). Завдяки цьому Cisco ASA здатна забезпечити надійний захист як від зовнішніх, так і від внутрішніх загроз, що робить її ідеальним вибором для великих організацій, які потребують комплексної мережевої безпеки.

Основною функцією Cisco ASA є забезпечення міжмережевого екрану, який перевіряє пакети на основі їхнього стану та історії з'єднань. Це дозволяє фільтрувати несанкціонований доступ і блокувати шкідливий трафік, що забезпечує високий рівень безпеки в корпоративних мережах. Завдяки цій функції Cisco ASA ефективно протидіє більшості зовнішніх атак і забезпечує захист від несанкціонованого проникнення.

Особливим додатковим елементом є інтеграція з Advanced Malware Protection (AMP), що дозволяє Cisco ASA виявляти та блокувати як відомі, так і невідомі загрози. Використання машинного навчання та аналізу поведінки дозволяє системі швидко реагувати на нові загрози, що з'являються в мережі. Ця інтеграція робить Cisco ASA сильним інструментом у боротьбі з кіберзагрозами, включаючи ті, що можуть бути новими або складними для виявлення традиційними методами.

Однією з функцій Cisco ASA є підтримка конфігурацій високої доступності (HA), таких як Active/Standby та Active/Active. Це дозволяє забезпечити безперервну роботу системи навіть у разі відмови одного з пристроїв, що є критичним для підприємств, які потребують стабільної роботи без перерв. Масштабованість Cisco ASA дозволяє їй ефективно справлятися зі збільшенням навантаження та зберігати високу продуктивність навіть при збільшенні кількості з'єднань та обсягу трафіку.

Інтеграція Cisco ASA з іншими рішеннями Cisco, такими як Cisco Identity Services Engine (ISE) та Cisco Umbrella, що дозволяє централізовано управляти політиками безпеки, забезпечуючи комплексний підхід до захисту корпоративних мереж. Інтеграція з цими системами забезпечує додаткові рівні захисту і дозволяє

здійснювати більш детальне керування доступом на основі ідентичності користувачів і пристроїв.

Загалом, Cisco ASA є надійним рішенням для забезпечення безпеки корпоративних мереж. Вона поєднує високий рівень захисту, гнучкість налаштувань, можливість інтеграції з іншими рішеннями безпеки та масштабованість, що робить її ідеальним вибором для великих організацій. Це рішення дозволяє не тільки ефективно захищати мережі від зовнішніх та внутрішніх загроз, але й адаптуватися до нових кіберзагроз, забезпечуючи безпеку даних і ресурсів в умовах швидко змінного кіберпростору.

Cisco ASA є надійним і багатофункціональним рішенням для забезпечення комплексної безпеки корпоративних мереж. Окрім базових функцій міжмережевого екрану та VPN, вона підтримує інтеграцію з передовими технологіями для виявлення загроз, таких як Cisco Firepower та Advanced Malware Protection (AMP). Це дозволяє значно розширити можливості з безпеки, здійснюючи детальний аналіз трафіку на рівні додатків і забезпечуючи захист від нових та складних загроз, таких як нульові вразливості або невідомі шкідливі програми.

Система підтримує не тільки традиційні методи захисту, але й адаптивні механізми для боротьби з новими викликами, що з'являються в умовах постійно змінюваного кіберпростору. Модульна архітектура пристрою дозволяє без проблем додавати нові функціональні модулі, зберігаючи високу гнучкість і масштабованість системи. Це робить Cisco ASA значущим інструментом для організацій, які стикаються з постійно зростаючими вимогами до безпеки.

Також варто зазначити, що Cisco ASA надає можливості для централізованого управління політиками безпеки через інтеграцію з іншими продуктами Cisco, такими як Cisco ISE (Identity Services Engine) та Cisco Umbrella. Це дозволяє адміністраторам більш ефективно керувати доступом до мережі, застосовуючи політики на основі ідентичності користувачів і пристроїв, а також забезпечувати додаткові рівні захисту від зовнішніх і внутрішніх загроз.

Завдяки підтримці високої доступності та конфігурацій Active/Standby і Active/Active, Cisco ASA забезпечує безперервну роботу системи навіть при відмові одного з пристроїв. Це критично важливо для підприємств, які вимагають стабільної і безперебійної роботи своїх мережевих ресурсів.

Таким чином, Cisco ASA є невід'ємним компонентом інфраструктури безпеки для великих підприємств, забезпечуючи надійний захист, високий рівень масштабованості та гнучкості, а також інтеграцію з передовими системами для виявлення і запобігання загрозам. Вона дозволяє організаціям ефективно протидіяти сучасним кіберзагрозам, захищати свої дані та ресурси і підтримувати безпечну роботу мережі на всіх етапах.

2.2. Використання Cisco ASA для контролю доступу та фільтрації трафіку

Списки контролю доступу (ACL) на Cisco ASA є одним із ключових інструментів реалізації політик безпеки, що дозволяють гнучко керувати доступом до корпоративних ресурсів. Вони дають змогу обмежувати доступ до мережі, дозволяючи підключатися лише певним користувачам, пристроям або системам, що значно підвищує рівень захисту інформаційних активів організації.

Cisco ASA підтримує різні типи ACL, що забезпечує широкий спектр можливостей фільтрації трафіку. Стандартні ACL дозволяють обмежувати доступ за IP-адресами джерела, що є простим, але ефективним способом контролю мережевого трафіку. Розширені ACL значно ширші за функціоналом: вони можуть фільтрувати трафік за IP-адресою, протоколом, портами, напрямком передачі, що дозволяє впроваджувати детальні політики безпеки, адаптовані до конкретних потреб організації. Іменовані ACL, у свою чергу, полегшують адміністрування, оскільки замість числових ідентифікаторів використовують зручні для сприйняття назви, що сприяє кращій організації та управлінню правилами доступу.

Після створення ACL їхні правила застосовуються безпосередньо до інтерфейсів ASA. Це забезпечує перевірку кожного пакету на відповідність

політикам безпеки під час проходження через пристрій. Такий підхід гарантує, що тільки дозволений трафік потрапить до внутрішньої мережі або до конкретних сегментів, у той час як заборонений буде ефективно блокований.

Особливу увагу Cisco ASA приділяє захисту самого пристрою. Для цього використовуються спеціальні ACL, які обмежують доступ до управлінських інтерфейсів, таких як SSH чи ASDM, дозволяючи підключення лише з довірених адрес. Це мінімізує ризики несанкціонованого доступу до системи керування, що є критично важливим для збереження цілісності та безпеки всієї мережевої інфраструктури.

Крім базової фільтрації, Cisco ASA має розвинуті функції моніторингу і логування трафіку. Адміністратори можуть отримувати детальну інформацію про всі спроби доступу, у тому числі несанкціоновані, що полегшує проведення розслідувань і оперативне реагування на інциденти. Логування дозволяє вести повний аудит подій, що є важливою складовою системи безпеки і відповідає вимогам багатьох стандартів і нормативів.

Ще одним значущим аспектом є підтримка налаштування VPN-з’єднань на Cisco ASA. Це дозволяє організувати захищений віддалений доступ до корпоративної мережі для працівників, віддалених офісів або партнерів. Шифрування VPN-трафіку гарантує конфіденційність і цілісність переданої інформації, захищаючи її від перехоплення або підробки.

Cisco ASA також підтримує фільтрацію трафіку на рівні додатків, що дозволяє застосовувати політики безпеки конкретно для програм і сервісів. Це дає змогу блокувати небажані або шкідливі додатки, мінімізуючи ризики, пов’язані з виконанням небезпечного коду або несанкціонованим доступом до мережевих ресурсів.

Щодо аутентифікації, Cisco ASA забезпечує інтеграцію з популярними сервісами централізованого управління доступом, такими як LDAP і RADIUS. Це дозволяє ефективно управляти правами користувачів і забезпечувати дотримання корпоративних політик безпеки, контролюючи, хто і з якими правами може підключатися до мережі.

Інтеграція з системами виявлення та запобігання вторгненням (IDS/IPS) розширює можливості ASA, дозволяючи виявляти і блокувати складні атаки в реальному часі. Ці системи моніторять мережевий трафік, аналізують поведінку пакетів і автоматично реагують на підозрілу активність, що значно знижує ризики успішного проникнення.

Також ASA підтримує впровадження політик якості обслуговування (QoS), що дає змогу пріоритезувати трафік критичних додатків і сервісів. Це особливо важливо у великих мережах, де одночасно працюють різні служби з різними вимогами до пропускної здатності та затримок.

Для полегшення керування ASA пропонує централізоване адміністрування через Cisco Adaptive Security Device Manager (ASDM) і інші автоматизовані інструменти, що дозволяє адміністраторам швидко і зручно налаштовувати і моніторити пристрої без складнощів.

Для захисту від розподілених атак на відмову в обслуговуванні (DDoS) Cisco ASA має спеціальні механізми, що допомагають зберегти доступність важливих ресурсів навіть у разі масштабних атак, що особливо актуально для великих підприємств.

Варто також відзначити високу масштабованість ASA, що дозволяє використовувати пристрої як у малих, так і у великих мережах, з можливістю інтеграції з хмарними сервісами і підтримкою різних типів з’єднань, що забезпечує гнучкість і адаптивність системи безпеки.

Інтеграція ASA з Cisco FirePOWER додає можливості глибшого аналізу трафіку – включно з фільтрацією за репутацією IP-адрес, контролем додатків і URL-фільтрацією. Це дозволяє виявляти і блокувати складні загрози, які можуть обходити звичайні методи фільтрації, що робить систему більш стійкою до сучасних атак.

Завдяки всім цим функціям Cisco ASA є одним із найефективніших і надійних рішень для комплексного захисту мережі на всіх рівнях, включаючи захист від зовнішніх атак, внутрішніх загроз і контроль доступу до критично важливих ресурсів організації.

2.3. Можливості інтеграції Cisco ASA з іншими засобами захисту

Інтеграція Cisco ASA з іншими засобами захисту кінцевих пристроїв дозволяє створити багаторівневу систему безпеки, яка забезпечує ефективний захист від сучасних кіберзагроз. Це досягається через обмін інформацією між ASA та рішеннями для захисту кінцевих пристроїв, такими як Cisco Secure Endpoint, Cisco Identity Services Engine (ISE), а також інтеграцію з платформами XDR та SIEM.

Одним із ключових компонентів сучасної системи безпеки є Cisco Secure Endpoint (раніше відомий як AMP for Endpoints), який надає розширені можливості для виявлення та запобігання вторгненням, аналізу поведінки додатків та управління вразливостями на кінцевих пристроях. Інтеграція Cisco ASA з Cisco Secure Endpoint дозволяє автоматично реагувати на інциденти безпеки в режимі реального часу: заражені пристрої миттєво ізолюються від мережі, а зловмисний трафік блокується. Це значно прискорює процес виявлення та реагування на загрози, мінімізуючи час, необхідний для відновлення нормального функціонування мережі після інцидентів.

Для централізованого управління політиками доступу та забезпечення відповідності корпоративним вимогам безпеки ASA інтегрується з Cisco Identity Services Engine (ISE). Цей інструмент дозволяє здійснювати гнучку автентифікацію та авторизацію користувачів і пристроїв, застосовуючи політики доступу на основі ролей і безпекового стану кінцевих пристроїв. Такий підхід дає можливість ASA динамічно адаптувати правила фільтрації трафіку відповідно до рівня довіри до кожного конкретного користувача чи пристрою, забезпечуючи більш точний контроль і захист мережі.

Інтеграція Cisco ASA з платформами розширеного виявлення і реагування (XDR), такими як Secureworks Taegis, Cortex XDR та Blumira, забезпечує передачу журналів подій і інформації про мережеві з’єднання для глибшого аналізу та кореляції загроз. Завдяки цьому можливе виявлення складних, прихованих атак, які можуть залишатися непоміченими при традиційних методах моніторингу. Також

забезпечується автоматичне реагування на виявлені інциденти, що підвищує загальну ефективність системи безпеки.

Для забезпечення захищеного віддаленого доступу Cisco ASA підтримує інтеграцію з рішеннями багатофакторної автентифікації, такими як Duo Security. Це дозволяє підвищити безпеку підключень до корпоративної мережі через VPN, запроваджуючи додаткові фактори автентифікації – наприклад, біометричні дані, одноразові коди або апаратні токени. Такий підхід значно знижує ризик несанкціонованого доступу навіть у разі компрометації основних облікових даних.

Крім того, використання MFA є важливою складовою архітектури нульової довіри (Zero Trust), де кожен доступ до ресурсів перевіряється динамічно, незалежно від того, чи перебуває користувач у внутрішній мережі, чи поза її межами. У цьому контексті Cisco ASA виступає як компонент, що забезпечує перевірку контексту доступу, взаємодіючи з системами автентифікації для блокування підозрілої активності, захисту від фішингу та інших сучасних атак, спрямованих на обхід традиційних методів автентифікації.

Впровадження багатофакторної автентифікації також допомагає компаніям дотримуватися вимог нормативних актів, таких як GDPR та HIPAA, які вимагають посилених заходів безпеки для захисту персональних і медичних даних. Використання Cisco ASA у поєднанні з такими рішеннями дозволяє підприємствам відповідати цим вимогам і знижувати ризики порушень безпеки.

Ще одним необхідним аспектом є підтримка ASA керованих політик безпеки на основі ролей (RBAC). Це дає адміністраторам змогу визначати, які користувачі чи групи мають доступ до конкретних мережевих ресурсів, а які – ні. Завдяки цьому реалізується принцип найменших привілеїв, що суттєво знижує ризики внутрішніх загроз та помилок користувачів.

Cisco ASA також інтегрується з рішеннями систем управління інформацією і подіями безпеки (SIEM), що забезпечує централізований моніторинг, збір і аналіз даних про безпеку у реальному часі на рівні всього підприємства. Це дозволяє оперативно виявляти аномальні дії і потенційні загрози, пришвидшуючи реагування і зменшуючи наслідки інцидентів.

Додатково, ASA підтримує автоматичне оновлення баз даних загроз і механізмів захисту, що забезпечує проактивний захист від новітніх кіберзагроз. Це дає змогу пристрою швидко адаптуватися до змін у кіберсередовищі, підтримуючи актуальність і ефективність заходів безпеки.

Завдяки комплексу цих функцій Cisco ASA забезпечує всебічний захист корпоративної мережі, дозволяючи організаціям ефективно захищати свої ресурси від широкого спектру загроз, зберігати високу продуктивність мережевої інфраструктури і одночасно підтримувати необхідну гнучкість для віддалених підключень користувачів.

На рис. 2.1 зображена схема можливої інтеграції Cisco ASA з іншими засобами захисту.

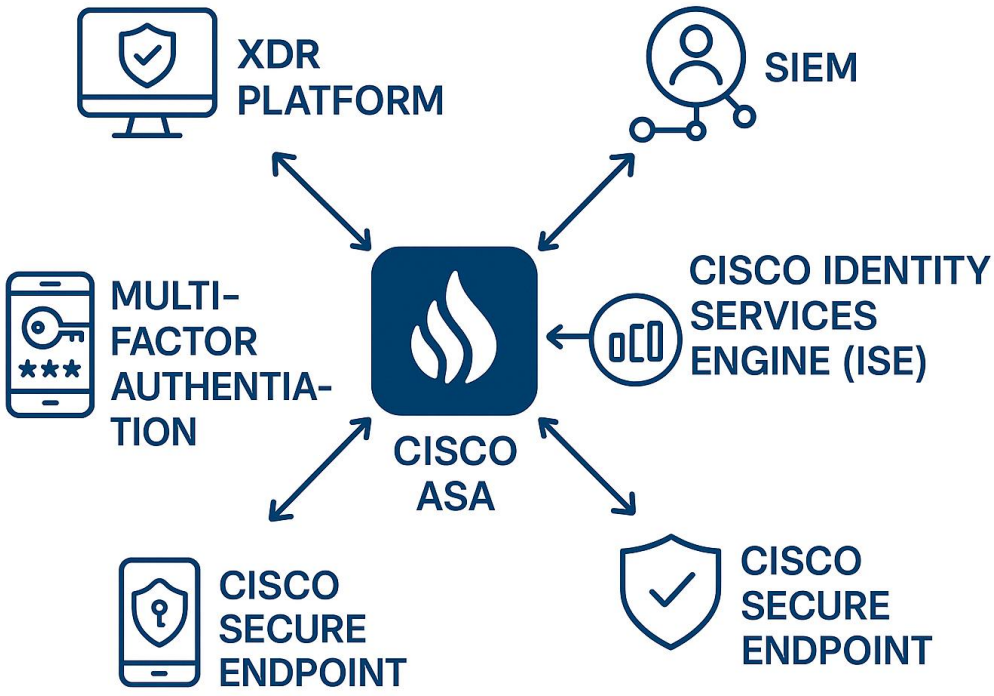

Рис. 2.1. Інтеграція Cisco ASA з іншими засобами захисту

Інтеграція Cisco ASA з іншими засобами захисту кінцевих пристроїв створює єдину централізовану систему безпеки, яка забезпечує комплексний захист від широкого спектра кіберзагроз. Такий підхід дає змогу організаціям ефективно управляти безпекою як мережі, так і кінцевих пристроїв, суттєво знижуючи ризики та підвищуючи рівень захисту своїх інформаційних ресурсів [2].

Ця інтеграція є ключовим кроком у формуванні багаторівневої системи безпеки, яка здатна ефективно протидіяти сучасним загрозам. Об’єднання Cisco ASA з рішеннями, такими як Cisco Secure Endpoint, Cisco Identity Services Engine (ISE), а також платформами для розширеного виявлення та реагування (XDR) і системами управління інформацією про безпеку (SIEM), значно підвищує ефективність виявлення атак і реакції на них.

Cisco Secure Endpoint забезпечує можливості для раннього виявлення вторгнень, аналізу поведінки додатків і запобігання атакам на кінцеві пристрої. Завдяки цій інтеграції ASA може автоматично ізолювати заражені пристрої та блокувати зловмисний трафік, що значно скорочує час відновлення роботи після інцидентів безпеки. Інтеграція з Cisco Identity Services Engine (ISE) додає можливість централізованої автентифікації та авторизації користувачів і пристроїв, при цьому застосовуються політики доступу на основі ролей та безпекового стану, що підвищує загальний рівень захищеності мережі.

Платформи XDR, такі як Secureworks Taegis, Cortex XDR і Blumira, надають глибший аналіз загроз, дозволяючи виявляти складні, багатошарові атаки, які можуть бути непомітними при використанні традиційних методів моніторингу. Завдяки цьому Cisco ASA стає частиною більш масштабної екосистеми безпеки, яка автоматично координує реагування на інциденти, підвищуючи загальну стійкість мережі.

Використання багатофакторної автентифікації, наприклад, через інтеграцію з Duo Security, додає ще один необхідний рівень захисту для користувачів, що підключаються до корпоративної мережі через VPN. Це значно покращує безпеку віддаленого доступу, зменшуючи ризики несанкціонованого проникнення навіть у випадках компрометації основних облікових даних.

Крім того, така централізована система безпеки сприяє більш ефективній координації дій між різними захисними компонентами, дозволяючи оперативно обмінюватися інформацією про загрози та реагувати на них у режимі реального часу. Це дозволяє значно зменшити час виявлення і локалізації атак, а також швидко впроваджувати контрзаходи, що мінімізує потенційні збитки для бізнесу.

Важливим аспектом є також можливість масштабування системи. Завдяки інтеграції різних рішень на базі Cisco ASA організації можуть поступово розширювати свій рівень захисту, додаючи нові компоненти і функціональні можливості без необхідності кардинальної перебудови існуючої інфраструктури.

Впровадження єдиної централізованої системи безпеки на базі Cisco ASA та супутніх рішень також полегшує дотримання нормативних вимог та стандартів у сфері інформаційної безпеки. Організації отримують можливість централізовано контролювати політики доступу, аудит безпеки та звітність, що є значущим для проходження перевірок і збереження репутації.

Загалом, інтегрована екосистема на базі Cisco ASA створює надійний, масштабований і адаптивний захист, який відповідає сучасним вимогам кібербезпеки та дозволяє організаціям впевнено працювати в умовах постійно змінних загроз. Це особливо актуально для підприємств із критично важливою інформацією, великими мережевими структурами та розгалуженими каналами віддаленого доступу.

Додатковою складовою інтегрованої системи безпеки є автоматизація процесів реагування на інциденти. Завдяки можливостям сучасних платформ, таких як Cisco SecureX, інтеграція Cisco ASA з іншими рішеннями дозволяє автоматично виявляти загрози, корелювати події безпеки та запускати відповідні контрзаходи без участі людини. Це значно підвищує швидкість реакції на кіберінциденти і мінімізує потенційні наслідки для бізнесу.

Ще одним перспективним напрямком розвитку є застосування технологій штучного інтелекту та машинного навчання у системах безпеки. Cisco ASA та супутні продукти активно впроваджують аналітику поведінки користувачів і пристроїв, що дозволяє передбачати і запобігати атакам на ранніх етапах. Використання таких технологій забезпечує проактивний захист і знижує навантаження на фахівців з кібербезпеки.

Важливим також є забезпечення високої доступності та стійкості системи. Cisco ASA підтримує різні архітектурні рішення для відмовостійкості, включаючи

кластеризацію і резервування, що гарантує безперервну роботу мережі навіть у випадку виходу з ладу окремих компонентів.

Окрім технічних аспектів, централізована система на базі Cisco ASA сприяє кращому управлінню політиками безпеки, стандартизації процедур і дотриманню вимог регуляторів. Це особливо потрібно для організацій, які працюють у сферах з підвищеними вимогами до безпеки інформації, таких як фінанси, охорона здоров’я та державний сектор.

Таким чином, подальший розвиток та впровадження інтегрованих систем безпеки на базі Cisco ASA створюють фундамент для захисту сучасних організацій від складних кіберзагроз, забезпечуючи баланс між ефективністю, надійністю і масштабованістю захисних механізмів.

3 РЕАЛІЗАЦІЯ ЗАХИСТУ КІНЦЕВИХ ПРИСТРОЇВ НА ОСНОВІ CISCO ASA

3.1. Розробка політик та правил в Cisco ASA для захисту кінцевих пристроїв

Розробка політик та правил в Cisco ASA для захисту кінцевих пристроїв є важливим етапом забезпечення мережевої безпеки в корпоративному середовищі.

Cisco ASA (Adaptive Security Appliance) являє собою багатофункціональний мережевий пристрій, який об’єднує можливості міжмережевого екрана зі станом з’єднання (Stateful Firewall), підтримку VPN, механізми трансляції мережевих адрес (NAT), систему виявлення вторгнень (IPS), а також засоби фільтрації трафіку. Пристрій забезпечує централізований захист мережі, контролює доступ до її ресурсів і спрямований на запобігання як зовнішнім, так і внутрішнім загрозам для кінцевих пристроїв.

Cisco ASA працює на базі принципу zone-based firewall, де мережеві інтерфейси поділяються на зони, такі як inside, outside, dmz. Кожній зоні відповідає певний рівень довіри. Наприклад, зона inside зазвичай має найвищий рівень довіри (100), а outside — найнижчий (0). Між цими зонами створюються політики, які визначають, який трафік дозволено чи заборонено.

На рис. 3.1 наведено типову схему сегментації мережі з використанням Cisco ASA:

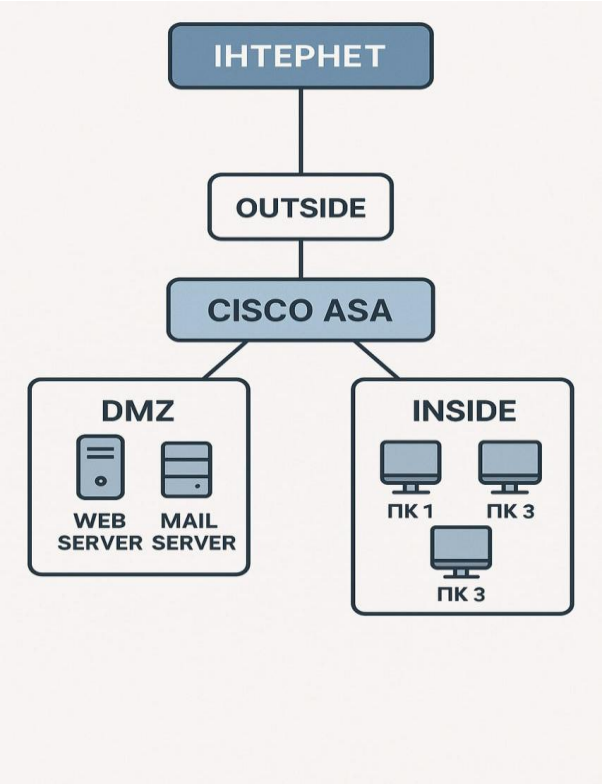

Рис. 3.1. Сегментації мережі з використанням Cisco ASA

На схемі видно, що Cisco ASA розміщується між корпоративною локальною мережею (inside) і мережею Інтернет (outside). Може також бути виділена зона DMZ для публічних серверів, таких як веб-сервер або поштовий сервер.

Політики доступу в Cisco ASA реалізуються через Access Control Lists (ACL), які дозволяють або забороняють певні типи трафіку між зонами [16]. Наприклад, щоб дозволити вихід HTTP/HTTPS трафіку з внутрішньої мережі до Інтернету, та заборонити все інше, використовується наступний блок команд у CLI:

ciscoasa# configure terminal

ciscoasa(config)# access-list OUTSIDE_IN extended permit tcp 192.168.10.0 255.255.255.0 any eq 80

ciscoasa(config)# access-list OUTSIDE_IN extended permit tcp 192.168.10.0 255.255.255.0 any eq 443

ciscoasa(config)# access-list OUTSIDE_IN extended deny ip any any

ciscoasa(config)# access-group OUTSIDE_IN in interface outside

Ці правила дозволяють доступ з внутрішнього сегменту 192.168.10.0/24 до портів 80 (HTTP) і 443 (HTTPS) у зовнішній мережі, та блокують увесь інший трафік.

Не менш важливою є конфігурація NAT (Network Address Translation), яка дозволяє кінцевим пристроям мати доступ до Інтернету з використанням єдиної зовнішньої IP-адреси. Для реалізації dynamic NAT можна використати такі команди [17]:

ciscoasa# configure terminal

ciscoasa(config)# object network obj-inside

ciscoasa(config-network-object)# subnet 192.168.10.0 255.255.255.0

ciscoasa(config-network-object)# nat (inside,outside) dynamic interface

Цей запис означає, що всі пристрої в мережі 192.168.10.0/24 будуть використовувати зовнішню адресу інтерфейсу ASA для виходу в Інтернет.

Для безпечного з’єднання віддалених офісів часто використовується VPN (Virtual Private Network). У Cisco ASA налаштування VPN передбачає створення списку доступу, що визначає дозволений трафік між локальними мережами [3]:

ciscoasa# configure terminal

ciscoasa(config)# access-list VPN_ACL extended permit ip 192.168.20.0 255.255.255.0 192.168.10.0 255.255.255.0

Цей ACL дозволяє передавання трафіку між віддаленою мережею 192.168.20.0/24 та локальною 192.168.10.0/24 через VPN-тунель.

Для забезпечення контролю та аналізу подій необхідно налаштувати логування:

ciscoasa# configure terminal

ciscoasa(config)# logging enable

ciscoasa(config)# logging trap notifications

ciscoasa(config)# logging host inside 192.168.10.100

ASA буде надсилати повідомлення з рівнем "notifications" на сервер логів у локальній мережі [20].

Щоб зберегти всі зміни у конфігурації після налаштування, використовується команда:

ciscoasa# write memory

Або:

ciscoasa# copy running-config startup-config

Для діагностики, наскільки певний пакет проходить через правила міжмережевого екрану, можна використовувати команду packet-tracer:

ciscoasa# packet-tracer input inside tcp 192.168.1.10 12345 8.8.8.8 80

Це дозволяє в режимі симуляції побачити, яке правило дозволить або заблокує даний пакет.

Додатково можна скористатися командами для моніторингу:

ciscoasa# show conn

ciscoasa# show access-list

ciscoasa# show run

Ці команди дозволяють переглядати активні з'єднання, статистику трафіку та поточну конфігурацію пристрою.

Для зручності в табл. 3.1 подано типи політик:

Табл. 3.1.

Типи політик

Тип політики	Призначення	Приклад реалізації
ACL	Контроль трафіку між зонами	access-list + access-group
NAT	Трансляція адрес внутрішньої мережі	object network + nat
VPN	Шифрування міжофісного трафіку	crypto map, tunnel-group
Тип політики	Призначення	Приклад реалізації
Логування	Моніторинг та аудит	logging enable, logging host
Packet inspection	Глибока перевірка трафіку (ASA MPF)	class-map, policy-map

У підсумку, якщо грамотно налаштувати Cisco ASA, він дає можливість не просто керувати тим, який трафік проходить через мережу, а й забезпечує надійний

захист пристроїв усередині від зовнішніх і внутрішніх загроз. Через нього можна відсіювати небажані підключення, вести запис подій для подальшого аналізу, а також безпечно з’єднувати офіси або філії через захищені канали. Усе це можливо лише за умови чіткого планування та правильного створення правил доступу і фільтрації, що в підсумку гарантує стабільну й захищену роботу всієї мережевої інфраструктури.

3.2. Розробка рекомендацій щодо впровадження рішення в інфраструктуру організації

Впровадження рішення на основі Cisco ASA (Adaptive Security Appliance) в інфраструктуру організації є стратегічно важливим кроком для підвищення рівня мережевої безпеки. Cisco ASA поєднує в собі функціональність міжмережевого екрана, системи запобігання вторгненням (IPS), VPN-шлюзу, а також механізми глибокого інспектування трафіку. Таке інтегроване рішення дозволяє організації забезпечити захист на периметрі мережі, реалізувати сегментацію внутрішнього трафіку та організувати безпечний віддалений доступ для співробітників і партнерів. Водночас ефективність впровадження залежить від правильної методології, що включає технічний аналіз, адаптацію політик безпеки, навчання персоналу та забезпечення безперервного моніторингу.

На табл. 3.2 продемонстровані етапи впровадження Cisco ASA в інфраструктуру організації [20].

Табл. 3.2

Етапи впровадження Cisco ASA в інфраструктуру організації.

№	Етап	Короткий опис
1	Аудит мережевої інфраструктури	Виявлення критичних вузлів, DMZ, аналіз потоків трафіку
2	Оцінка сумісності та розробка PoC	Перевірка архітектурної інтеграції з наявним обладнанням
3	Створення зон безпеки та ACL	Формування правил доступу, ізоляція DMZ, визначення пріоритетів

Продовження табл. 3.2

4	Впровадження VPN та MFA	Організація захищених тунелів для віддалених користувачів
5	Навчання адміністраторів	Підготовка до роботи з CLI, ASDM, журналами, моніторингом
6	Моніторинг і кореляція подій	Інтеграція з SIEM, аналіз аномалій, автоматизоване реагування
7	Забезпечення високої доступності	Налаштування кластерів HA, резервне копіювання, тестування на відмовостійкість

Першим етапом має стати детальний аудит IT-інфраструктури, зокрема мережевої топології, маршрутизації, активного обладнання, а також поточних точок контролю трафіку. Особливу увагу слід приділити існуючим маршрутам, правилам доступу, конфігураціям VLAN, зонам DMZ та серверам, що мають вихід в Інтернет. На основі результатів аудиту формується уявлення про точки інтеграції Cisco ASA, необхідність використання одного чи кількох пристроїв, обсяг необхідного ліцензування та рівень складності сегментації.

Далі здійснюється оцінка сумісності Cisco ASA з існуючими мережевими рішеннями, включаючи маршрутизатори, комутатори, балансувальники навантаження та VPN-клієнти. Варто враховувати, що ASA може бути інтегрована як у класичну модель мережі (core-distribution-access), так і в більш гнучкі архітектури з віртуальними мережами. У випадку використання хмарних або гібридних моделей, рекомендовано додатково оцінити доцільність впровадження віртуального рішення Cisco ASAv [5]. Для малих і середніх організацій можливе впровадження фізичного пристрою з обмеженою кількістю інтерфейсів, тоді як для великих підприємств доцільна кластеризація ASA з резервуванням високої доступності.

На етапі проєктування конфігурації особливу увагу слід приділити створенню зон безпеки та правил між ними. Cisco ASA оперує концепцією security levels, яка визначає рівень довіри до інтерфейсів (наприклад, inside=100, dmz=50, outside=0). Це дозволяє задавати політики доступу з урахуванням контексту

трафіку. Наприклад, користувачі з внутрішньої мережі можуть ініціювати з'єднання із зовнішніми ресурсами, але не навпаки. Важливим елементом є налаштування Access Control Lists (ACLs), які дозволяють обмежити трафік на основі IP-адрес, портів, протоколів і навіть прикладного рівня (залежно від функціоналу ASA).

Окрему увагу варто приділити організації DMZ-зони. Рекомендується винести публічно доступні ресурси (веб-сервери, поштові шлюзи, DNS-сервери) у сегмент, ізольований як від зовнішньої мережі, так і від внутрішньої. Це дозволяє мінімізувати ризики у разі компрометації сервісу. ASA дає змогу гнучко управляти трафіком між DMZ та іншими зонами за допомогою ACL та фільтрації на рівні прикладного протоколу.

Наступним кроком є впровадження механізмів VPN. Cisco ASA підтримує як IPsec VPN для site-to-site-з’єднань, так і SSL VPN для клієнтського доступу. Це дає змогу організувати захищений канал для віддалених співробітників, інтегрувати філії компанії та підтримувати мобільність. При цьому важливо реалізувати багатофакторну автентифікацію (MFA), яка може бути налаштована через інтеграцію з Cisco Duo або іншими сервісами [22]. Крім того, VPN-з'єднання мають бути обмежені за часом, IP-діапазонами та перевіркою пристрою клієнта.

Критичним елементом є оновлення політик безпеки. Організація має адаптувати свої правила доступу, вимоги до журналювання, сегментацію доступу та розслідування інцидентів. Cisco ASA дозволяє створювати детальні журнали подій, які можуть бути інтегровані в SIEM-системи, такі як Splunk, QRadar або Azure Sentinel [19]. Це відкриває можливості для кореляції подій, виявлення аномалій та реагування в реальному часі. Для підвищення ефективності бажано також активувати механізми Threat Detection, які автоматично виявляють підозрілу активність і можуть заблокувати джерело атаки [8].

Навчання персоналу – один з обов’язкових етапів впровадження Cisco ASA. Адміністраторам слід надати документацію щодо команд CLI, принципів роботи з ASDM (ASA Device Manager) або Firepower Management Center (у разі використання моделі з інтегрованим IPS). Кінцевим користувачам необхідно

пояснити нові вимоги до з'єднань, VPN-доступу та дій у разі обмежень з боку міжмережевого екрана.

Після впровадження рішення слід налаштувати постійний моніторинг ефективності. Це включає регулярний перегляд журналів, аналіз підозрілих з'єднань, звітність про блоковані атаки, виявлення сканувань портів, аналіз трафіку на наявність ботнет-активності. Рекомендується встановити базові метрики: кількість зафіксованих спроб вторгнення, середній час реагування, частота оновлень політик, кількість заблокованих з'єднань на рівні DMZ. Впровадження Cisco ASA має також супроводжуватись планом регулярного тестування політик, включаючи пенетраційне тестування, оцінку сегментації та аудит змін конфігурації.

На завершальному етапі доцільно формалізувати процедури взаємодії з зовнішніми провайдерами (наприклад, у разі використання віддаленого адміністрування або хостингу частини сервісів). Необхідно чітко визначити SLA, розподіл зон відповідальності, політики реагування на інциденти та резервне відновлення. Cisco ASA підтримує налаштування failover-кластерів, що дозволяє забезпечити безперервність обслуговування навіть у разі виходу з ладу основного пристрою.

Таким чином, впровадження рішення Cisco ASA повинно бути сплановане з урахуванням не лише технічних параметрів пристрою, а й вимог безпеки, бізнес-процесів, відповідності стандартам та гнучкої адаптації до нових викликів. За умови правильного підходу Cisco ASA здатне стати надійною основою периметрового захисту організації.

3.3. Оцінка ефективності запропонованого рішення

Оцінювання ефективності впровадженого мережевого захисту на базі Cisco ASA є критично важливим етапом, що дозволяє не лише перевірити правильність реалізації політик, а й визначити реальний вплив рішення на безпеку та працездатність інформаційної інфраструктури. Цей процес має бути

систематичним, заснованим на метриках, які охоплюють як технічні, так і організаційні аспекти.

Зокрема, ефективність визначається за такими ключовими критеріями, як зниження кількості атак і небажаного трафіку, покращення часу виявлення та реагування на інциденти, наявність детальних журналів подій і можливість їх кореляції. Важливу роль відіграють також стабільність роботи сервісів та здатність системи мінімізувати кількість хибнопозитивних спрацювань, а також помірне навантаження на ресурси інфраструктури.

На практиці ефективність рішення можна потенційно вимірювати за допомогою таких метрик:

Табл. 3.2

Метрики для оцінки ефективності Cisco ASA

Метрика	До впровадження	Після впровадження	Коментар
Час виявлення загрози (MTTD)	6 годин	< 15 хвилин	Завдяки інтеграції з SIEM і глибокому аналізу
Кількість успішних атак на DMZ	3 на місяць	0	Сегментація і ACL ефективно ізолюють DMZ
Середній час реагування (MTTR)	> 2 годин	~20 хвилин	Використання автоматизованих дій
Наявність повного журналювання подій	Часткове	Повне	Всі спроби доступу реєструються
Інциденти через несанкціонований доступ	4 на квартал	0	MFA і VPN – контроль обмежують доступ

Ще один підхід до оцінки – аналіз змін у потоках реагування на інциденти. Порівняння стану до та після реалізації рішення ілюструє зміни в якості реагування.

Наступна табл. 3.3, демонструє трансформацію ключових процесів забезпечення інформаційної безпеки в організації до і після впровадження рішення на базі Cisco ASA у поєднанні з SIEM-системою. Вона містить п’ять основних

аспектів, які характеризують рівень зрілості захисту: виявлення, реакцію, журналювання, аналіз і ризики.

Табл 3.3

Шляхи реагування до і після впровадження Cisco ASA

До впровадження	Після впровадження
Виявлення – вручну через лог-файли	Виявлення – автоматично через SIEM + ASA
Реакція – з затримкою, вручну	Реакція – автоматизована або напівавтоматична
Журналювання – неповне	Журналювання – централізоване та повне
Аналіз – постфактум	Аналіз – у реальному часі з кореляцією
Ризик пропуску загрози – високий	Ризик пропуску загрози – мінімальний

Таку ключову роль відіграє сумісність рішень Cisco з іншим програмно-апаратним забезпеченням. Позитивний ефект спостерігається особливо у випадках, коли була впроваджена централізована система моніторингу на базі SIEM або NOC/SOC, що дозволяє корелювати події, відстежувати вразливості та застосовувати проактивні заходи реагування [2].

Для візуалізації повного ефекту інтеграції представлено діаграму типового сценарію після впровадження на рис. 3.4

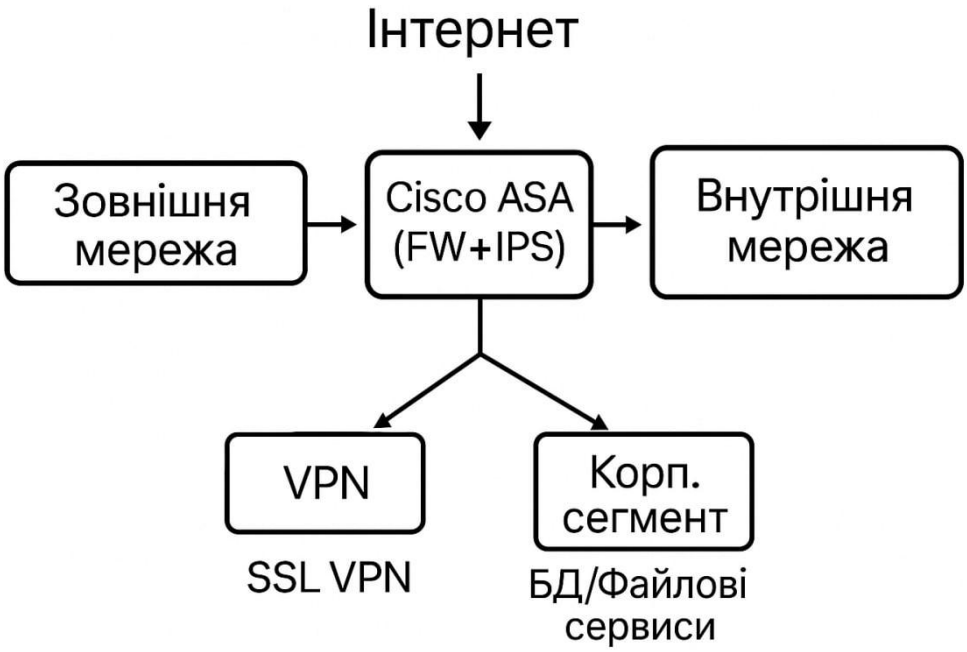

Рис. 3.4. Сценарій взаємодії компонентів після впровадження Cisco ASA

Цей рисунок ілюструє архітектуру мережевої взаємодії після впровадження Cisco ASA, показуючи як пристрій виступає центральним вузлом безпеки між зовнішнім середовищем та внутрішніми ресурсами організації [7].

Також важливо враховувати організаційні аспекти ефективності:

- Чітке документування політик;
- Проведення тренінгів для адміністраторів;
- Внутрішній аудит змін у правилах;
- Використання механізмів ревізії та SIEM-кореляції.

Впроваджене рішення має не лише технічну перевагу, а й формує культуру безпеки: адміністраторам зрозуміло, як аналізувати інциденти, користувачі усвідомлюють обмеження доступу, а керівництво отримує звітність для прийняття рішень на основі ризиків.

У підсумку, ефективність реалізованого рішення визначається зменшенням площі можливої атаки, підвищенням прозорості трафіку в мережі, скороченням часу реагування на інциденти, а також появою можливостей для прогнозування потенційних загроз. Таким чином, Cisco ASA, за умови правильної інтеграції, не

лише знижує кількість потенційних загроз, а й дозволяє своєчасно виявляти аномалії, забезпечуючи прийняття зважених рішень у сфері реагування на кіберінциденти.

Таким чином, Cisco ASA, при умові правильної інтеграції, не лише зменшує кількість потенційних загроз, а й дозволяє оперативно виявляти аномалії та приймати зважені рішення у сфері реагування.

ВИСНОВКИ

У межах проведеного дослідження було виконано всебічний аналіз проблеми захисту кінцевих пристроїв в організаційній інфраструктурі, що є актуальним завданням у сучасному кіберпросторі. Кінцеві точки залишаються одними з найуразливіших елементів мережі, оскільки мають прямий доступ до конфіденційних ресурсів і часто стають початковою точкою для кібератак. На основі вивчення поточних загроз і моделей атак було виокремлено ключові напрямки забезпечення захисту, серед яких — фільтрація трафіку, застосування правил доступу, шифрування даних, інтеграція з SIEM та впровадження багатофакторної автентифікації.

У рамках технічної реалізації захисту було обґрунтовано доцільність використання Cisco ASA як основного компонента мережевої безпеки. Це рішення дозволяє впроваджувати зонну модель з різними рівнями довіри, створювати детальні ACL, реалізовувати VPN-доступ, а також вести централізоване журналювання подій. У ході практичного моделювання було продемонстровано, що правильне налаштування ASA значно зменшує ризик зовнішніх атак і спрощує контроль внутрішнього трафіку. Окрема увага приділялася зв’язці Cisco ASA з іншими засобами безпеки, що дозволяє забезпечити не лише захист периметра, але й підтримку безпеки кінцевих точок у контексті цілісної архітектури.

Оцінювання ефективності впровадження Cisco ASA показало суттєве покращення основних показників безпеки. Серед позитивних результатів — зменшення часу виявлення інцидентів, підвищення повноти журналювання, зниження кількості порушень у зоні DMZ, а також зростання прозорості дій користувачів. Інтеграція з системами типу SIEM і платформами MFA дозволила автоматизувати виявлення загроз і зменшити навантаження на фахівців. Поряд із цим виявлено, що ефективне використання Cisco ASA вимагає належного рівня підготовки адміністраторів, актуалізації політик безпеки та періодичного аудиту конфігурацій.

У перспективі система на базі Cisco ASA може бути ефективно розширена шляхом:

- інтеграції з платформами автоматизованого реагування на інциденти (SOAR);
- впровадження архітектури Zero Trust;
- застосування машинного аналізу поведінки користувачів;
- переходу до хмарної або гібридної моделі розгортання засобів захисту.

У підсумку можна стверджувати, що Cisco ASA є ефективним, адаптивним та масштабованим рішенням для забезпечення мережевої безпеки й захисту кінцевих точок. Його використання дозволяє істотно зменшити ризики компрометації, посилити контроль доступу та сформувати надійну основу для побудови цілісної системи захисту в умовах постійно змінюваних кіберзагроз.

ПЕРЕЛІК ПОСИЛАНЬ

1. Безпека кінцевих точок і сучасна відповідність. URL: https://lazarusalliance.com/uk/endpoint-security-and-modern-compliance/ (Дата звернення: 20.05.2025).

2. How to To-The-Box Traffic Filtering on Cisco ASA. URL: https://community.cisco.com/t5/network-security/how-to-to-the-box-traffic-filtering-on-cisco-asa/td-p/4493968 (Дата звернення: 20.05.2025).

3. Cisco ASA Integration Guide. URL: https://docs.taegis.secureworks.com/integration/connectNetwork/cisco_connect/ (Дата звернення: 20.05.2025).

4. Integrating with Cisco ASA Firewall. URL: https://support.blumira.com/hc/en-us/articles/5015498640659-Integrating-with-Cisco-ASA-Firewall (Дата звернення: 20.05.2025).

5. Configuration Guides. URL: https://www.cisco.com/c/en/us/support/security/adaptive-security-appliance-asa-software/products-installation-and-configuration-guides-list.html (Дата звернення: 20.05.2025).

6. Cisco ASA ACL Best Practices and Examples | Auvik. URL: https://www.auvik.com/franklyit/blog/acls-cisco-asa-firewalls/ (Дата звернення: 20.05.2025).

7. Single Sign-On for Cisco ASA with Secure Client | Duo Security. URL: https://duo.com/docs/sso-ciscoasa (Дата звернення: 20.05.2025).

8. ASDM Book 3: Cisco Secure Firewall ASA Series VPN ASDM Configuration Guide, 7.19. URL: ASDM Book 3: Cisco Secure Firewall ASA Series VPN ASDM Configuration Guide, 7.19 (Дата звернення: 20.05.2025).

9. Assess Endpoint Compliance Using Cisco Secure Client ISE Posture Module and Cisco Secure Firewall Management Center. URL: Assess Endpoint Compliance Using Cisco Secure Client ISE Posture Module and Cisco Secure Firewall Management Center (Дата звернення: 20.05.2025).

10. Cisco Firewall Best Practices. URL: Cisco Firewall Best Practices (Дата звернення: 20.05.2025).

11. Solutions - Cisco Secure Endpoint At a Glance. URL: Solutions - Cisco Secure Endpoint At a Glance (Дата звернення: 20.05.2025).

12. Писарчук, О. О., & Кошара, А. В. (2024). АНАЛІЗ ІНДИКАТОРІВ ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ ЗА РЕЗУЛЬТАТАМИ ЗАСТОСУВАННЯ SIEM-СИСТЕМ. *Інфокомунікаційні та комп'ютерні технології*, *1*(07), 79-84. URL: https://doi.org/10.36994/2788-5518-2024-01-07-11 (Дата звернення: 20.05.2025).

13. Cisco Secure Endpoint - Configuration Examples and TechNotes. URL: Cisco Secure Endpoint - Configuration Examples and TechNotes (Дата звернення: 20.05.2025).

14. Cisco Secure Endpoint (Formerly AMP for Endpoints). URL: Cisco Secure Endpoint (Formerly AMP for Endpoints) (Дата звернення: 20.05.2025).

15. Managing Secure Firewall ASA with Security Cloud Control - Get Started. URL: Managing Secure Firewall ASA with Security Cloud Control - Get Started (Дата звернення: 20.05.2025).

16. Мережеве DLP vs. DLP для кінцевих точок. URL: https://corewin.ua/blog/network-dlp-vs-endpoint-dlp (Дата звернення: 20.05.2025).

17. Endpoint Protection 2025: огляд кращих рішень для корпоративної безпеки. URL: https://softlist.com.ua/ua/news/endpoint-protection-oglyad-krashchih-rishen-dlya-korporativnoyi-bezpeki (Дата звернення: 20.05.2025).

18. Top 10 Endpoint Security Solutions for 2025. URL: https://www.sentinelone.com/cybersecurity-101/endpoint-security/endpoint-security-solutions/ (Дата звернення: 20.05.2025).

19. Endpoint Protection - Enterprise Software. URL: https://www.softwarereviews.com/categories/endpoint-protection-enterprise (Дата звернення: 20.05.2025).

20. Захист кінцевих точок: як не загубитися у різноманітті продуктів. URL: https://trellix.bakotech.com/home/endpoint-protection-how-not-to-get-lost-in-the-variety-of-products (Дата звернення: 20.05.2025).

21. Захист комп'ютерних мереж за допомогою AC L- списків. URL: https://theslide.ru/uncategorized/zahist-kompyuternih-merezh-za-dopomogoyu-as (Дата звернення: 20.05.2025).

22. Cisco ASA Access-List. URL: https://networklessons.com/cisco/asa-firewall/cisco-asa-access-list (Дата звернення: 20.05.2025).